The MacWilliams Theorem for Four-Dimensional Modulo Metrics

Mehmet Özen, Murat Güzeltepe
Department of Mathematics, Sakarya University, TR54187 Sakarya, Turkey

Abstract

In this paper, the MacWilliams theorem is stated for codes over finite field with four-dimensional modulo metrics.

AMS Classification: 94B05, 94B60
Keywords: MacWilliams theorem, Block codes, Weight enumerator, Quaternion Mannheim metric.

1 Introduction

The MacWilliams theorem is one of the most important theorems in coding theory. It is well known that two of the most famous results in block code theory are MacWilliams Identity Theorem end Equivalence Theorem [1, 2]. Given the weight enumerator of an code, the MacWilliams theorem ensure one to obtain the weight enumerator of the dual code . The MacWilliams theorem very useful since weight distribution of high rate codes can be obtained from low rate codes. A well known version of the MacWilliams theorem for codes with respect to Hamming weight was presented in [3]. The more general version of this theorem are less often used in practical applications. The impact of this theorem for practical as well as theoretical purposes is well known, see for instance [3, Chs. 11.3, 6.5, and 19.2]. In [4], the MacWilliam theorem proved for codes over finite fields with two-dimensional modulo metric.

In this study, we utilize the MacWilliam theorem for complete weight enumerators to obtain the MacWilliams theorem for codes over quaternion integers (QI). The Hamilton quaternion algebra is defined as follows.

Definition 1 *Let $\mathcal{R}$ be the field of real numbers. The Hamilton Quaternion Algebra over $\mathcal{R}$ denoted by $H[\mathcal{R}]$ is the associative unital algebra given by the following representation:*

i)$H[\mathcal{R}]$ is the free $\mathcal{R}$ module over the symbols $1, i, j, k$, that is, $H[\mathcal{R}] = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in R\}$;
ii)1 is the multiplicative unit;
iii) $i^2 = j^2 = k^2 = -1$;
iv) $ij = -ji = k$, $ik = -ki = j$, $jk = -kj = i$ [5].

If $q = a_0 + a_1 i + a_2 j + a_3 k$ is a quaternion integer, its conjugate quaternion is $\overline{q} = a_0 - (a_1 i + a_2 j + a_3 k)$. The norm of q is $N(q) = q.\overline{q} = a_0^2 + a_1^2 + a_2^2 + a_3^2$, which is multiplicative, that is, $N(q_1 q_2) = N(q_1)N(q_2)$. It should be noted that quaternions are not commutative. The ring of the integers of the quaternions is $H[\mathcal{Z}] = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in \mathcal{Z}\}$. Let $H[\mathcal{Z}]_\pi$ be residue class of $H[\mathcal{Z}]$ modulo π, where π is prime quaternion integer. The set obtained form the elements of $H[\mathcal{Z}]_\pi$ obtains the elements which by the remainders from right dividing (or left dividing) the elements of $H[\mathcal{Z}]$ by the element π. For example, let $p = 3, \pi = 1 + i + j$ then we get $H[\mathcal{Z}]_\pi = \{\mp 1, \mp i, \mp j, \mp k\}$. Also $H[\mathcal{Z}]_\pi$ has $N(\pi)^2$ elements [6]. More information which is related with the arithmetic properties of $H[\mathcal{Z}]$ can be found in [5, pp. 57-71]. The quaternion Mannheim metric also called Lipschitz metric was defined in [6, 7]. Let $\alpha - \beta \equiv \delta = a_0 + a_2 i + a_2 j + a_3 k \pmod{\pi}$. Then the weight of δ which is denoted by $w_{QM}(\delta)$ is equal $|a_0| + |a_2| + |a_2| + |a_3|$. The distance between α and β was defined as $d_{QM}(\alpha, \beta) = w_{QM}(\delta)$.
Now we recall some notation and definitions on characters and weight enumerators needed in this paper. Let γ be an element of the Galois field $GF(p^m)$. Using the primitive element α, γ can be represented as $\gamma = \sum_{t=0}^{m-1} g_t \alpha^t$ with g_t from $GF(p)$. The character $\chi_1(\gamma)$ is defined using the primitive complex $p-th$ root ξ:

$$\chi_1(\gamma) = \xi^{g_0}$$

where $\xi = \exp(2\pi\sqrt{-1}/p)$, $\pi = 3,14...$
The complete weight enumerator classifies the codewords of a linear code according to the number of times each field element ω_t appears in the codeword. The composition of a vector $u = (\ u_0,\ \ u_1,\ \ \cdots\ \ , u_{n-1}\ )$ denoted by $comp(u)$ is given by $s = (\ s_0,\ \ s_1,\ \ \cdots\ \ , s_{q-1}\ )$, where s_t is the number of components u_t equal to ω_t. Note that there exist a group homomorphism between $GF(p^2)$ and $H[\mathcal{Z}]_\pi$ using a rational mapping. For example, assume that $p = 3$ then $\pi = 1 + i + j$, $GF(p^2) = \{0, 1, \alpha, \alpha^2, ..., \alpha^7\}$ and $H[\mathcal{Z}]_\pi = \{0, 1, -1, i, -i, j, -j, k, -k\}$ where $\alpha^2 = \alpha + 1$, $\alpha^8 = 1$. We obtain a group homomorphism mapping 0 to 0, 1 to 1, α to i, 2α to $-i$, $2 + 2\alpha$ to j, $1 + \alpha$ to $-j$, $2\alpha + 1$ to k, $\alpha + 2$ to $-k$.

Definition 2 *The composition of* $u = (\ u_0,\ \ u_1,\ \ \cdots\ \ , u_{n-1}\ )$*, denoted by* $comp(u)$*, is* $s = (\ s_0,\ \ s_1,\ \ \cdots\ \ s_{q-1}\ )$ *where* $s_t = s_t(u)$ *is the number of components* u_t *equal to* ω_t*. Thus it is obtain*

$$\sum_{t=0}^{q-1} s_t(u) = n.$$

Let C *be a linear* $[n, k]$ *code over* $GF(p)$*. Then the complete weight enumerator of* C

$$W_C(z_0, z_1, \cdots, z_{q-1}) = \sum_{c \in C} \left(\prod_{t=0}^{q-1} z_t^{s_t(u)} \right)$$

where z_t *are indeterminates and the sum extends over all compositions.*

The MacWilliams theorem for complete weight enumerators [3, pp.143-144, Thm 10] then states:

Theorem 1 *The complete weight enumerator of the dual code $C^{\perp}$ can be obtained from the complete weight enumerator of the code C by replacing each z_t by*

$$\sum_{s=0}^{q-1} \chi_1(\omega_t \omega_s) z_s$$

and dividing the result by the cardinality of C which is denoted by $|C|$.

2 The MacWilliams Theorem for codes over Quaternion Integers

Let $GF(q)$ be a finite field with $q = p^m$. The field $GF(q)$ is partitioned as follows:

$$GF(q) = \{0\} \cup G_1 \cup G_2 \cup G_3 \cup G_4 \cup G_5 \cup G_6 \cup G_7 \cup G_8.$$

We set $\omega_0 = 0$. G_1 contains $(q-1)/8$ elements ω_t, $t = 1, 2, ..., (q-1)/8$ in a fixed way such that for $t = 1, 2, ..., (q-1)/8$ we have

$$\begin{array}{l} G_2 = \omega_2 G_1,\ \omega_2 \notin G_1, \\ G_3 = \omega_3 G_1,\ \omega_3 \notin G_1 \cup G_2, \\ G_4 = \omega_4 G_1,\ \omega_4 \notin G_1 \cup G_2 \cup G_3, \\ G_5 = \omega_5 G_1,\ \omega_5 \notin G_1 \cup G_2 \cup G_3 \cup G_4, \\ G_6 = \omega_6 G_1,\ \omega_6 \notin G_1 \cup G_2 \cup G_3 \cup G_4 \cup G_5, \\ G_7 = \omega_7 G_1,\ \omega_7 \notin G_1 \cup G_2 \cup G_3 \cup G_4 \cup G_5 \cup G_6, \\ G_8 = \omega_8 G_1,\ \omega_8 \notin G_1 \cup G_2 \cup G_3 \cup G_4 \cup G_5 \cup G_6 \cup G_7. \end{array} .$$

The quaternion Mannheim weight of a vector u over $GF(p)$ is defined as $quaternionic(u) = \begin{pmatrix} g_0, & g_1, & \cdots & , g_{(q-1)/8} \end{pmatrix}$. Note that the quaternion integer enumerator does not distinguish between the eight elements $\mp\omega, \mp i\omega, \mp j\omega, \mp k\omega$. The complete weight enumerator of the dual code $C^{\perp}$ from the complete weight enumerator of the code C over $H[\mathcal{Z}]_{\pi}$ obtained as follows:

Theorem 2 *The quaternion integer (QI) weight enumerator of the dual code $C^{\perp}$ can be obtained from QI weight enumerator of C by replacing z_1 by*

$$z_0 + \sum_{s=1}^{(q-1)/8} \left[\begin{array}{l} \chi_1(\omega_1\omega_s) + \chi_1(-\omega_1\omega_s) + \chi_1(i\omega_1\omega_s) + \chi_1(-i\omega_1\omega_s) + \chi_1(j\omega_1\omega_s) \\ +\chi_1(-j\omega_1\omega_s) + \chi_1(k\omega_1\omega_s) + \chi_1(-k\omega_1\omega_s) \end{array} \right] z_s = z_0 +$$

$$[\chi_1(\omega_1\omega_1) + \chi_1(-\omega_1\omega_1) + \chi_1(i\omega_1\omega_1) + \chi_1(-i\omega_1\omega_1) + \chi_1(j\omega_1\omega_1) + \chi_1(-j\omega_1\omega_1) + \chi_1(k\omega_1\omega_1) + \chi_1(-k\omega_1\omega_1)] z_1 + \cdots$$

$$+ \left[\begin{array}{l} \chi_1(\omega_1\omega_{(q-1)/8}) + \chi_1(-\omega_1\omega_{(q-1)/8}) + \chi_1(i\omega_1\omega_{(q-1)/8}) + \chi_1(-i\omega_1\omega_{(q-1)/8}) + \chi_1(j\omega_1\omega_{(q-1)/8}) \\ +\chi_{(q-1)/8}(-j\omega_1\omega_{(q-1)/8}) + \chi_1(k\omega_1\omega_{(q-1)/8}) + \chi_1(-k\omega_1\omega_{(q-1)/8}) \end{array} \right] z_{(q-1)/8},$$

z_2 *by*

$$[\chi_1(\omega_1\omega_1) + \chi_1(-\omega_1\omega_1) + \chi_1(i\omega_1\omega_1) + \chi_1(-i\omega_1\omega_1) + \chi_1(j\omega_1\omega_1) + \chi_1(-j\omega_1\omega_1) + \chi_1(k\omega_1\omega_1) + \chi_1(-k\omega_1\omega_1)] z_2 + \cdots$$

$$+ \left[\begin{array}{l} \chi_1(\omega_1\omega_{(q-1)/8}) + \chi_1(-\omega_1\omega_{(q-1)/8}) + \chi_1(i\omega_1\omega_{(q-1)/8}) + \chi_1(-i\omega_1\omega_{(q-1)/8}) + \chi_1(j\omega_1\omega_{(q-1)/8}) \\ +\chi_{(q-1)/8}(-j\omega_1\omega_{(q-1)/8}) + \chi_1(k\omega_1\omega_{(q-1)/8}) + \chi_1(-k\omega_1\omega_{(q-1)/8}) \end{array} \right] z_1 ...$$

and using the same argument, shifting the coefficients of $z_1, z_2, \cdots, z_{(q-1)/8}$, $z_{(q-1)/8}$ *by*

$$[\chi_1(\omega_1\omega_1)+\chi_1(-\omega_1\omega_1)+\chi_1(i\omega_1\omega_1)+\chi_1(-i\omega_1\omega_1)+\chi_1(j\omega_1\omega_1)+\chi_1(-j\omega_1\omega_1)+\chi_1(k\omega_1\omega_1)+\chi_1(-k\omega_1\omega_1)]z_{(q-1)/8}$$

$$+\left[\begin{array}{l}\chi_1(\omega_1\omega_{(q-1)/8})+\chi_1(-\omega_1\omega_{(q-1)/8})+\chi_1(i\omega_1\omega_{(q-1)/8})+\chi_1(-i\omega_1\omega_{(q-1)/8})+\chi_1(j\omega_1\omega_{(q-1)/8})\\ +\chi_{(q-1)/8}(-j\omega_1\omega_{(q-1)/8})+\chi_1(k\omega_1\omega_{(q-1)/8})+\chi_1(-k\omega_1\omega_{(q-1)/8})\end{array}\right]z_{((q-1)/8)-}$$

The proof is immediately obtained from MacWilliams theorem for complete weight enumerators above.

Example 1 *Let* $p = 3$, $\pi = 1+i+j+k$. *Then* $H[\mathcal{Z}]_\pi = \{0, 1, -1, i, -i, j, -j, k, -k\}$. *Let us consider* $[2, 1, 2]$ *- code* C *over* $GF(9) = H[\mathcal{Z}]_\pi$. *Thus we get* $GF(9) = H[\mathcal{Z}]_\pi = G_0 \cup G_1 = \{0\} \cup \{\mp 1, \mp i, \mp j, \mp k\}, \omega_0 = 0,\ \omega_1 = 1$ *Assume that the code* C *which is an left ideal of* $H[\mathcal{Z}]_\pi \times H[\mathcal{Z}]_\pi$ *is generate by the matrix* $(1, 1)$. *Then the complete weight enumerator of* C *is* $w_{QM}(C) = z_0^2 + 8z_1^2$. *Applying the QI MacWilliams theorem means that to replace* $z_1 \to z_0 + \left(\xi^1 + \xi^2 + \xi^0 + \xi^0 + \xi^2 + \xi^1 + \xi^1 + \xi^2\right) z_1 = z_0 - z_1$. $1 + \xi^1 + \xi^2 = 0$ *since there is a group homomorphism between* $GF(p^2)$ *and* $H[\mathcal{Z}]_\pi$, *where* $\xi = e^{2\pi i/3}$, $\pi = 3, 14...$ *Thus the complete weight enumerator of the dual code* $C^\perp$ *is equal* $z_0^2 + 8z_1^2 = w_{QM}(C)$.

Example 2 *Let* $p = 5$, $\pi = 2 + i$. *Then*

$$H[\mathcal{Z}]_\pi = \{0\} \cup \{1, -1, i, -i, j, -j, k, -k\} \cup (1 + j)\{1, -1, i, -i, j, -j, k, -k\}$$
$$\cup (1 + k)\{1, -1, i, -i, j, -j, k, -k\}.$$

Let us consider $[3, 1, 3]$*-code over* $GF(25) = H[\mathcal{Z}]_{2+i}$. *Thus we get,* $\omega_0 = 0$, $\omega_1 = 1$, $\omega_2 = 1 + \alpha \leftrightarrow 1 + j$, $\omega_3 = 1 + 2\alpha \leftrightarrow 1 + k$. *Assume that the code* C *which is an left ideal of* $H[\mathcal{Z}]_\pi \times H[\mathcal{Z}]_\pi$ *is generate by the matrix* $\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$. *Then the complete weight enumerator of* C *is* $w_{QM}(C) = z_0^3 + 8z_1^3 + 8z_2^3 + 8z_3^3$. *Applying the QI MacWilliams theorem means that to replace*

$$z_0 \to z_0 + 8z_1 + 8z_2 + 8z_3,$$

$$\begin{gathered} z_1 \to z_0 + (\xi^1 + \xi^4 + \xi^3 + \xi^2 + \xi^0 + \xi^0 + \xi^0 + \xi^0)z_1 + \\ +(\xi^1 + \xi^4 + \xi^4 + \xi^1 + \xi^3 + \xi^2 + \xi^2 + \xi^3)z_2 \\ +(\xi^1 + \xi^4 + \xi^4 + \xi^1 + \xi^3 + \xi^2 + \xi^2 + \xi^3)z_3, \end{gathered}$$

$$\begin{gathered} z_2 \to z_0 + (\xi^1 + \xi^4 + \xi^3 + \xi^2 + \xi^0 + \xi^0 + \xi^0 + \xi^0)z_2 + \\ +(\xi^1 + \xi^4 + \xi^4 + \xi^1 + \xi^3 + \xi^2 + \xi^2 + \xi^3)z_3 \\ +(\xi^1 + \xi^4 + \xi^4 + \xi^1 + \xi^3 + \xi^2 + \xi^2 + \xi^3)z_1, \end{gathered}$$

$$\begin{gathered} z_3 \to z_0 + (\xi^1 + \xi^4 + \xi^3 + \xi^2 + \xi^0 + \xi^0 + \xi^0 + \xi^0)z_3 + \\ +(\xi^1 + \xi^4 + \xi^4 + \xi^1 + \xi^3 + \xi^2 + \xi^2 + \xi^3)z_1 \\ +(\xi^1 + \xi^4 + \xi^4 + \xi^1 + \xi^3 + \xi^2 + \xi^2 + \xi^3)z_2. \end{gathered}$$

$1+\xi^1+\xi^2+\xi^3+\xi^4=0$ *since there is a group homomorphism between* $GF(5^2)$ *and* $H[\mathcal{Z}]_{2+i}$*, where* $\xi=e^{2\pi i/5}$, $\pi=3,14...$ *Thus the complete weight enumerator of the dual code* $C^{\perp}$ *is equal*

$$\begin{gathered} z_0^3+24z_0z_1^2+24z_0z_2^2+24z_0z_3^2+24z_1^3+24z_2^3+24z_3^3 \\ +48z_1^2z_2+48z_1z_2^2+48z_2z_3^2+48z_1^2z_3+48z_1z_3^2+48z_2^2z_3 \\ +192z_1z_2z_3. \end{gathered}$$

3 Conclusion

In this paper, we proved the MacWilliams for four-dimensional modulo metrics. In fact, the quaternion Mannheim metric can be seen as a four-dimensional generalization of the Lee metric. Also the quaternion Mannheim metric can be seen as a four-dimensional generalization of the Mannheim metric. In other words, if four-dimensional space is restricted to two-dimensional space then results in [4] are obtained.

References

[1] F. J. MacWilliams, "Combinatorial Problems of Elementary Abelian Groups," Ph.D. dissertation, Harvard Univ., Cambridge, MA, 1962.

[2] F. J. MacWilliams, "A theorem on the distribution of weights in a systematic code," Bell Syst. Tech. J., vol. 42, pp. 79-94, 1963.

[3] F. J. Macwilliams and N. J. Sloane, "The Theory of Error Correcting Codes", North Holland Pub. Co., 1977.

[4] K. Huber, "The MacWilliams Theorem for Two-Dimensional Modulo Metrics," AAECC, 41-48, 1997. (submitted, 2009).

[5] G. Davidoff, P. Sarnak, A. Valette, "Elementary Number Theory, Group Theory, Ramanujan Graphs", Cambridge University Pres, 2003.

[6] C. Martinez et al. "Perfect Codes from Cayley Graphs over Lipschitz Integers," IEEE Trans. Inform.Theory, vol. 55, pp. 3552-3562, August, 2009.

[7] M. zen and M. Gzeltepe, "Codes over Quaternion Integers", e-print arXiv:0905.4160v1.